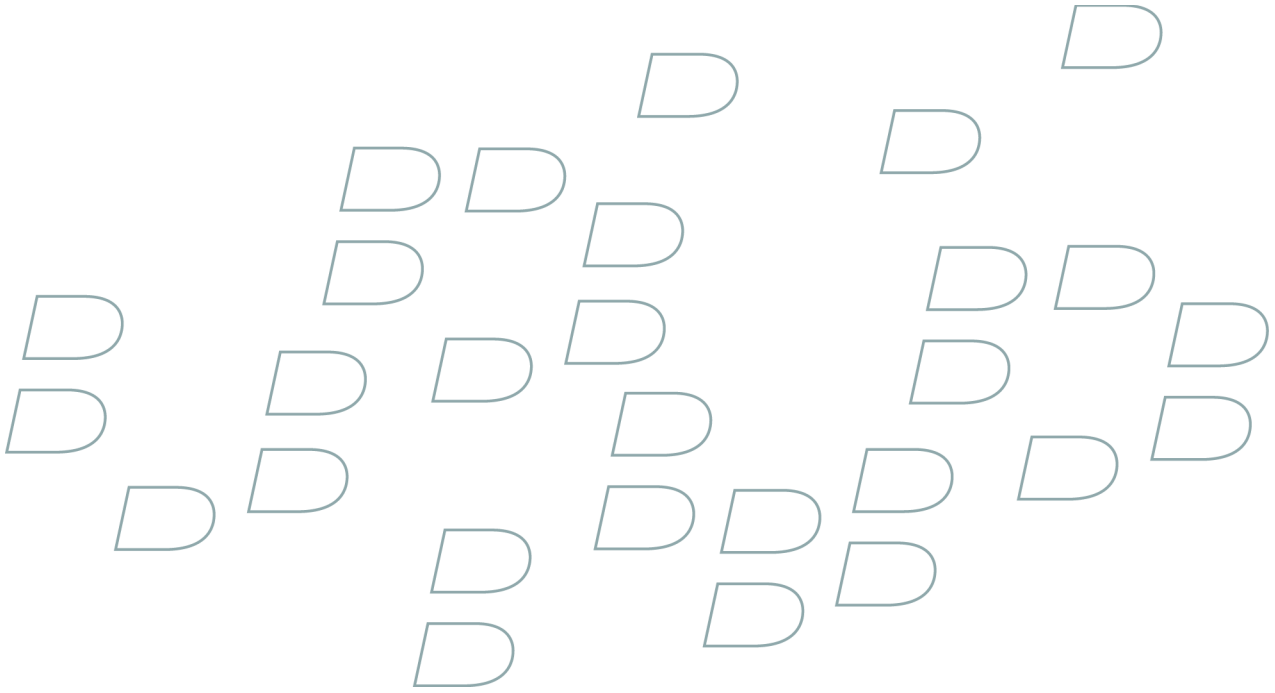

User Guide Supplement

S/MIME Support Package for BlackBerry Smartphones

BlackBerry 8800 Series

BlackBerry Curve 8300 Series

Contents

Certificates

Certificate basics

Download a certificate from an LDAP certificate server

1. In the device options, click **Security Options**.
2. Click **Certificates**.
3. Press the **Menu** key.
4. Click **Fetch Certificates**.
5. Specify the search criteria.
6. Press the **Menu** key.
7. Click **Search**.
8. Click a certificate.
9. Click **Add Certificate to Key Store**.

View properties for a certificate

1. In the device options, click **Security Options**.
2. Click **Certificates**.
3. Click a certificate.

Certificate properties

Revocation Status:
This field displays the revocation status of the certificate at a specified date and time.

Trust Status:
This field displays the trust status of the certificate chain. A certificate can be explicitly trusted (the certificate itself is trusted), implicitly trusted (the root certificate in the certificate chain is trusted on your BlackBerry® device), or not trusted (the certificate is not explicitly trusted and the root certificate in the certificate chain is not trusted or does not exist on your device).

Expiration Date:
This field displays the date that the certificate issuer specified as the expiration date of the certificate.

Certificate Type:
This field displays the certificate format. Your device supports X.509 and WTLS certificate formats.

Public Key Type:

This field displays the standard to which the public key complies. Your device supports RSA®, DSA, Diffie-Hellman, and ECC keys.

Subject:
This field displays information about the certificate subject.

Issuer:
This field displays information about the certificate issuer.

Serial Number:
This field displays the certificate serial number in hexadecimal format.

Key Usage:
This field displays approved uses of the public key.

Subject Alt Name:
This field displays an alternate email address for the certificate subject, if an alternate email address is available.

SHA1 Thumbprint:
This field displays the SHA-1 digital thumbprint of the certificate.

MD5 Thumbprint:
This field displays the MD5 digital thumbprint of the certificate.

View one type of certificate in the certificate list

1. In the device options, click **Security Options**.
2. Click **Certificates**.
3. Press the **Menu** key.
4. Click one of the following menu items:
   - **Show My Certs**
   - **Show Others Certs**
   - **Show CA Certs**
   - **Show Root Certs**

To view all the certificates on your BlackBerry® device, press the **Menu** key. Click **Show All Certs**.

Send a certificate

When you send a certificate, your BlackBerry® device sends the public key, but does not send the corresponding private key.

1. In the device options, click **Security Options**.
2. Click **Certificates**.
3. Highlight a certificate.
4. Press the **Menu** key.
5. Click **Send via Email** or **Send via PIN**.

Delete a certificate

1. In the device options, click **Security Options**.
2. Click **Certificates**.
3. Highlight a certificate.
4. Press the **Menu** key.
5. Click **Delete**.

View the certificate chain for a certificate

1. In the device options, click **Security Options**.
2. Click **Certificates**.
3. Highlight a certificate.
4. Press the **Menu** key.
5. Click **Show Chain**.

Certificate status

Certificate status indicators

 :

The certificate has a corresponding private key that is stored on your BlackBerry® device or a smart card.

 :

The certificate chain is trusted and valid, and the revocation status of the certificate chain is good.

 :

The revocation status of the certificate chain is unknown, or a public key for a certificate in the certificate chain is weak.

 :

The certificate is untrusted or revoked, or a certificate in the certificate chain is untrusted, revoked, expired, not valid, or cannot be verified.

Check the revocation status of a certificate or certificate chain

1. In the device options, click **Security Options**.
2. Click **Certificates**.
3. Highlight a certificate.
4. Press the **Menu** key.

5. Click **Fetch Status** or **Fetch Chain Status**.

Change the trust status of a certificate

1. In the device options, click **Security Options**.
2. Click **Certificates**.
3. Highlight a certificate.
4. Press the **Menu** key.
5. Click **Trust** or **Distrust**.
6. If necessary, perform one of the following actions:
   - To trust the highlighted certificate, click **Selected Certificate**.
   - To trust the highlighted certificate and all the other certificates in the chain, click **Entire Chain**.

Revoke a certificate

If you revoke a certificate, the certificate is revoked only in the key store on your BlackBerry® device. Your device does not update the revocation status on the certificate authority or CRL servers.

1. In the device options, click **Security Options**.
2. Click **Certificates**.
3. Highlight a certificate.
4. Press the **Menu** key.
5. Click **Revoke**.
6. Click **Yes**.
7. Change the **Reason** field.
8. Click **OK**.

To cancel a certificate hold, highlight the certificate. Press the **Menu** key. Click **Cancel Hold**.

Certificate revocation reasons

Unknown:
The revocation reason does not match any of the predefined reasons.

Key Compromise:
A person who is not the key subject might have discovered the private key value.

CA Compromise:
Someone might have revealed the private key of the certificate issuer.

Change in Affiliation:
The certificate subject no longer works for the organization.

Superseded:
A new certificate is replacing an existing certificate.

Cessation of Operation:
The certificate subject no longer requires the certificate.

Certificate Hold:
You want to revoke the certificate temporarily.

Certificate options

Change the display name for a certificate

1. In the device options, click **Security Options**.
2. Click **Certificates**.
3. Highlight a certificate.
4. Press the **Menu** key.
5. Click **Change Label**.
6. Type a display name for the certificate.
7. Click **OK**.

Add an email address to a certificate

1. In the device options, click **Security Options**.
2. Click **Certificates**.
3. Highlight a certificate.
4. Press the **Menu** key.
5. Click **Associate Addresses**.
6. Click the trackball.
7. Click **Add Address**.
8. Perform one of the following actions:
   - Click a contact.
   - Click **Use Once**. Type an email address. Click the trackball.
9. Press the **Menu** key.
10. Click **Save**.

Turn off the display name prompt that appears when you add a certificate to the key store

1. In the device options, click **Security Options**.
2. Click **Certificates**.

3. Press the **Menu** key.
4. Click **Fetch Certificates**.
5. Press the **Menu** key.
6. Click **Options**.
7. Change the **Prompt for Label** field to **No**.
8. Press the **Menu** key.
9. Click **Save**.

When you add a certificate, your BlackBerry® device uses the certificate subject as the name for the certificate.

Turn off the fetch status prompt that appears when you add a certificate to the key store

1. In the device options, click **Security Options**.
2. Click **Certificates**.
3. Press the **Menu** key.
4. Click **Fetch Certificates**.
5. Press the **Menu** key.
6. Click **Options**.
7. Perform one of the following actions:
   - To download the revocation status of a certificate when you add it to the key store, change the **Fetch Status** field to **Yes**.
   - To add a certificate to the key store without downloading the revocation status, change the **Fetch Status** field to **No**.
8. Press the **Menu** key.
9. Click **Save**.

Certificate shortcuts

- To view the certificate issuer, press the **Space** key.
- To view the properties of a certificate, press the **Enter** key.
- To view the security level of a certificate, press the **Alt** key and **L**.
- To view the serial number of a certificate, press the **Alt** key and **S**.
- To view certificates for certificate authorities, press the **Alt** key and **C**.
- To view personal certificates and certificates for other people, press the **Alt** key and **E**.
- To view personal certificates, press the **Alt** key and **P**.
- To view certificates for other people, press the **Alt** key and **O**.
- To view root certificates, press the **Alt** key and **R**.
- To view all certificates, press the **Alt** key and **A**.

Certificate troubleshooting

I cannot download a certificate

If you changed the connection type that your BlackBerry® device uses to connect to the LDAP certificate server, try switching to the default connection type.

Certificate servers

Add a certificate server

1. In the device options, click **Security Options**.
2. Click **Certificate Servers**.
3. Press the **Menu** key.
4. Click **New Server**.
5. Specify information for the certificate server.
6. Press the **Menu** key.
7. Click **Save**.

Change connection information for a certificate server

1. In the device options, click **Security Options**.
2. Click **Certificate Servers**.
3. Highlight a certificate server.
4. Press the **Menu** key.
5. Click **Edit**.
6. Change connection information for the certificate server.
7. Press the **Menu** key.
8. Click **Save**.

Connection options for LDAP certificate servers

Friendly Name:
Type a display name for the certificate server.

Server Name:
Type the network address of the certificate server.

Base Query:
Type the base query information for the certificate server using X.509 certificate syntax (for example, o=test.rim.net).

Port:
Type the port number for your organization's network. The default port number is 389.

Authentication Type:
Specify whether you must log in to the certificate server.

Connection Type:
Specify whether your BlackBerry® device uses an SSL connection or a TLS connection to connect to the certificate server.

Connection options for OCSP and CRL servers

Friendly Name:
Type a display name for the certificate server.

Server URL:
Type the web address of the certificate server.

Send connection information for a certificate server

1. In the device options, click **Security Options**.
2. Click **Certificate Servers**.
3. Highlight a certificate server.
4. Press the **Menu** key.
5. Click **Email Server** or **PIN Server**.

Delete a certificate server

1. In the device options, click **Security Options**.
2. Click **Certificate Servers**.
3. Highlight a certificate server.
4. Press the **Menu** key.
5. Click **Delete**.

Key stores

About the key store

The key store on your BlackBerry® device might store the following items. To access these items in the key store, you must type a key store password.

- personal certificates (certificate and private key pairs)
- certificates that you download using the certificate synchronization tool of the BlackBerry® Desktop Manager
- certificates that you download from an LDAP certificate server
- certificates that you add from a message
- personal PGP® keys (public and private key pairs)
- PGP public keys that you download from an LDAP certificate server
- PGP public keys that you add from a message
- root certificates that are included in the BlackBerry® Desktop Software

Change the key store password

1. In the device options, click **Security Options**.
2. Click **Key Stores**.
3. Press the **Menu** key.
4. Click **Change Password**.

Change when your device deletes the key store password

1. In the device options, click **Security Options**.
2. Click **Key Stores**.
3. Change the **Private Key Password Timeout** field.
4. Press the **Menu** key.
5. Click **Save**.

To access private keys after your BlackBerry® device deletes the key store password, you must type your key store password.

Add contacts to your address book automatically when you add items to the key store

1. In the device options, click **Security Options**.
2. Click **Key Stores**.

3. Change the **Key Store Address Injector** field to **Enabled**.
4. Press the **Menu** key.
5. Click **Save**.

Change the service that your device uses to download certificates

Depending on your organization, you might not be able to change the service that you use to download certificates. For more information, contact your administrator.

1. In the device options, click **Security Options**.
2. Click **Key Stores**.
3. Change the **Certificate Service** field.
4. Press the **Menu** key.
5. Click **Save**.

Turn off automatic backup of key store data

By default, items in the key store on your BlackBerry® device are backed up or restored when you back up or restore your device data. If you do not want to back up your private key to or restore your private key from your computer for security reasons, you can turn off automatic backup and restore of key store data.

1. In the device options, click **Security Options**.
2. Click **Key Stores**.
3. Change the **Allow Key Store Backup/Restore** field to **No**.
4. Press the **Menu** key.
5. Click **Save**.

To turn on automatic backup of key store data, change the **Allow Key Store Backup/Restore** field to **Yes**.

Change the refresh rate for certificate revocation lists

1. In the device options, click **Security Options**.
2. Click **Key Stores**.
3. Change the **Certificate Status Expires After** field.
4. Press the **Menu** key.
5. Click **Save**.

Your BlackBerry® device downloads a new revocation status automatically when your device uses a key store item with a status that is older than the time limit that you set.

Reject certificate revocation lists from unverified CRL servers

1. In the device options, click **Security Options**.

2. Click **Key Stores**.
3. Change the **Accept Unverified CRLs** field to **No**.
4. Press the **Menu** key.
5. Click **Save**.

Your BlackBerry® device rejects certificate revocation lists from CRL servers that the BlackBerry® MDS Connection Service cannot verify.

S/MIME-protected messages

S/MIME-protected message basics

About signing and encrypting messages

You can digitally sign or encrypt messages to add another level of security to email messages and PIN messages that you send from your BlackBerry® device. Digital signatures are designed to help recipients verify the authenticity and integrity of messages that you send. When you digitally sign a message using your private key, recipients use your public key to verify that the message is from you and that the message has not been changed.

Encryption is designed to keep messages confidential. When you encrypt a message, your device uses the recipient's public key to encrypt the message. Recipients use their private key to decrypt the message.

To send an encrypted PIN message, you must have a PIN and an email address for the contact in your address book. Your device uses the email address in your address book to locate a PGP® key or certificate for the contact.

Sign or encrypt a message

You can sign or encrypt email messages and PIN messages.

1. When composing a message, change the **Encoding** field.
2. If necessary, change the **Classification** field.

Attach a certificate to a message

You can attach a certificate to email messages and PIN messages.

1. When composing a message, press the **Menu** key.
2. Click **Attach Certificates**.
3. Highlight a certificate.
4. Press the **Menu** key.
5. Click **Continue**.

Download the certificate used to sign or encrypt a message

If a certificate is not included in a received message or is not already stored in the key store on your BlackBerry® device, you can download the certificate.

1. In a message, highlight the encryption indicator or a digital signature indicator.
2. Press the **Menu** key.
3. Click **Fetch Sender's Certificate**.

Add a certificate from a message

1. In a message, highlight a digital signature indicator.
2. Press the **Menu** key.
3. Click **Import Sender's certificate**.

Add a certificate from an attachment

1. In a message, click the certificate attachment.
2. Click **Retrieve Certificate Attachment**.
3. Click the certificate.
4. Click **Import Certificate**.

Add connection information for a certificate server from a message

1. In a message, highlight the certificate server indicator.
2. Click the trackball.
3. Click **Import Server**.

View the certificate used to sign or encrypt a message

1. In a message, highlight the encryption status indicator or a digital signature indicator.
2. Click the trackball.
3. Click **Display Sender's Certificate** or **Display Encryption Certificate**.

View encryption information for a weakly encrypted message

1. In a weakly encrypted message, highlight the encryption status indicator.
2. Press the **Menu** key.
3. Click **Encryption Details**.

S/MIME-protected message status

Digital signature indicators

 :
Your BlackBerry® device verified the digital signature.

 :

Your device cannot verify the digital signature.

 :

Your device requires more data to verify the digital signature.

 :

Your device trusts the certificate chain.

 :

The sender's email address does not match the email address of the certificate subject, or the sender's certificate is revoked, is not trusted, cannot be verified , or is not on your device.

 :

The certificate is weak, the certificate status is not current, or your device requires more data to verify the trust status of the certificate.

 :

The sender's certificate is expired.

Encryption status indicators

Your administrator sets whether messages that you receive are considered to be strong or weak.

 :

The message is strongly encrypted.

 :

The message is weakly encrypted.

Check the status of a certificate or certificate chain

If a certificate is included in a received message, or is already stored in the key store on your BlackBerry® device, you can check the status of the sender's certificate, or you can check the status of the sender's certificate and all other certificates in the certificate chain.

1. In a message, highlight a digital signature indicator.
2. Press the **Menu** key.
3. Click **Check Sender's Certificate** or **Check Sender's Cert Chain**.

S/MIME-protected message options

Change your signing or encryption certificate

Your BlackBerry® device uses your encryption certificate to encrypt messages in the sent items folder and includes your encryption certificate in messages that you send so that recipients can encrypt their reply messages.

1. In the device options, click **Security Options**.
2. Click **S/MIME**.
3. In the **Signing Options** section or the **Encryption Options** section, change the **Certificate** field.
4. Press the **Menu** key.
5. Click **Save**.

Change the default signing and encryption option

Your BlackBerry® device is designed to use the default signing and encryption option when you send a message to a contact that you have not sent a message to or received a message from previously. If you have sent a message to or received message from the contact previously, your device tries to use the signing and encryption option that was used for the last message.

1. In the device options, click **Advanced Options**.
2. Click **Default Services**.
3. Change the **Default Encoding** field.
4. Press the **Menu** key.
5. Click **Save**.

About message classifications

If your BlackBerry® device is associated with an email account that uses a BlackBerry® Enterprise Server that supports this feature and your administrator turns on message classifications, the BlackBerry Enterprise Server applies a minimum set of security actions to each message that you compose, forward, or reply to, based on the classification that you assign to the message. Your administrator specifies the message classifications that you can use.

If you receive a message that uses message classifications, you can view the abbreviation for the classification in the subject line of the message and the full description for the classification in the body of the message. You can also view the abbreviation and full description for the classification for a sent message in the sent items folder.

Change the default message classification

Verify that your administrator has turned on message classifications.
Your BlackBerry® device is designed to use the default message classification when you send a message to a contact that you have not sent a message to or received a message from previously. If you have sent a message to or received message from the contact previously, your device tries to use the message classification that was used for the last message.

1. In the device options, click **Advanced Options**.
2. Click **Default Services**.
3. Change the **Default Classification** field.
4. Press the **Menu** key.
5. Click **Save**.

Change the size of S/MIME indicators in messages

1. In the device options, click **Security Options**.
2. Click **S/MIME**.
3. Change the **Message Viewer Icons** field.
4. Press the **Menu** key.
5. Click **Save**.

Change the encryption algorithms for S/MIME-protected messages

If a message has multiple recipients, your BlackBerry® device uses the first selected encryption algorithm in the list that all recipients are known to support.

1. In the device options, click **Security Options**.
2. Click **S/MIME**.
3. Select the check box beside one or more encryption algorithms.
4. Press the **Menu** key.
5. Click **Save**.

Request delivery notification for signed S/MIME-protected messages

1. In the device options, click **Security Options**.
2. Click **S/MIME**.
3. Change the **Request S/MIME Receipts** field to **Yes**.
4. Press the **Menu** key.
5. Click **Save**.

Turn off the prompt that appears before an S/MIME-protected message is truncated

1. In the device options, click **Security Options**.
2. Click **S/MIME**.
3. Change the **Warn about truncated messages** field to **No**.
4. Press the **Menu** key.
5. Click **Save**.

To turn on the prompt again, change the **Warn about truncated messages** field to **Yes**.

Turn off the prompt that appears when you use an S/MIME certificate that is not recommended for use

1. In the device options, click **Security Options**.
2. Click **S/MIME**.

3. Change the **Warn about problems with my certificates** field to **No**.
4. Press the **Menu** key.
5. Click **Save**.

To turn on the prompt again, change the **Warn about problems with my certificates** field to **Yes**.

S/MIME-protected message troubleshooting

Some signing and encryption options are not available on my device

Try performing the following actions:

- Verify that the email account that you are using supports all signing and encryption options.
- If you use message classifications, verify that the message classification supports the signing or encryption options that you want. Try using a different message classification.

I cannot open an attachment in an encrypted message

The attachment information might not be available on the BlackBerry® Enterprise Server, your administrator might have set options to prevent you from opening attachments in encrypted messages, or you might have received the message from an email account that does not support attachments in encrypted messages.

You cannot open an attachment in a PGP® protected message that was encrypted using the OpenPGP format by an IBM® Lotus Notes® client working with PGP® Desktop Professional or that was encrypted by the PGP® Universal Server.

Smart cards

About using a smart card with your device

Smart cards store certificates and private keys. You can use a smart card reader to import certificates from a smart card to the key store on your BlackBerry® device, but you cannot import private keys. As a result, private key operations such as signing and decryption use the smart card, and public key operations such as verification and encryption use the public certificates on your device.

If you use a smart card certificate to authenticate to your device, after you connect your smart card reader to your device, your device requests authentication from the smart card each time that you unlock your device.

If the S/MIME Support Package for BlackBerry® devices is installed on your device, you can use smart card certificates to send S/MIME-protected messages.

Import a certificate from a smart card

1. In the device options, click **Security Options**.
2. Click **Certificates**.
3. Press the **Menu** key.
4. Click **Import Smart Card Certs**.
5. Type your smart card password.
6. Select the check box beside a certificate.
7. Click **OK**.
8. Type your key store password.
9. Click **OK**.